



(12)发明专利申请

(10)申请公布号 CN 106971108 A

(43)申请公布日 2017. 07. 21

(21)申请号 201710165815.9

(22)申请日 2017.03.20

(71)申请人 郑州云海信息技术有限公司

地址 450000 河南省郑州市郑东新区心怡
路278号16层1601室

(72)发明人 孙玉军

(51)Int.Cl.

G06F 21/57(2013.01)

G06F 9/445(2006.01)

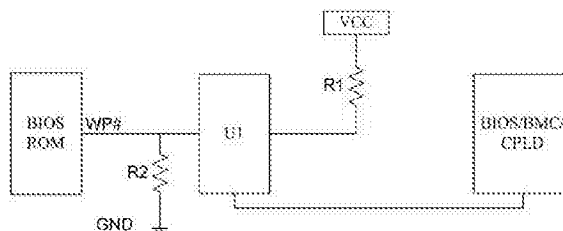
权利要求书1页 说明书2页 附图1页

(54)发明名称

一种在线更新BIOS的ROM写保护的系统及方法

(57)摘要

本发明公开了一种在线更新BIOS的ROM写保护的系统及方法,系统包括,依次连接的电源端VCC、第一电阻R1、开关模块U1、第二电阻R2、地端GND。BIOS的ROM的写保护管脚WP#连接于开关模块U1和第二电阻R2之间。开关模块U1与控制器件连接,并能根据控制器件的指令控制第一电阻R1、第二电阻R2的连接或断开。第一电阻R1与第二电阻R2分压能使写保护管脚WP#处于无效状态。其方法是通过控制开关模块的通断进而使写保护管脚WP#脚位,在不影响在线维护和DEBUG的基础上,使BIOS的ROM大部分时间处于写保护状态,不被操作指令误擦除或者写入,保持ROM文件的完整,提升系统稳定性,解决因为BIOS的ROM被改写或者擦除引起的不开机故障。



1. 一种在线更新BIOS的ROM写保护的系统,其特征在于,包括依次连接的电源端VCC、第一电阻R1、开关模块U1、第二电阻R2、地端GND;BIOS的ROM的写保护管脚WP#连接于开关模块U1和第二电阻R2之间;开关模块U1与控制器件连接,并能根据控制器件的指令控制第一电阻R1、第二电阻R2的连接或断开;第一电阻R1与第二电阻R2分压能使写保护管脚WP#处于无效状态。

2. 如权利要求1所述的优选的,在线更新BIOS的ROM写保护的系统,其特征在于,所述开关模块默认U1为断开状态。

3. 如权利要求1所述的优选的,在线更新BIOS的ROM写保护的系统,其特征在于,所述控制器件是BIOS、BMC、CPLD中的一种。

4. 如权利要求1所述的优选的,在线更新BIOS的ROM写保护的系统,其特征在于,所述第一电阻R1阻值为1k欧姆,第二电阻R2阻值为20k欧姆。

5. 根据权利要求1的一种在线更新BIOS的ROM写保护的方法,其特征在于,在正常使用中,开关模块U1断开,BIOS的ROM的写保护管脚WP#通过第二电阻R2接地;需要写BIOS的ROM时,控制器件发出中断请求信号,使开关模块U1导通,此时写保护管脚WP#通过第一电阻R1和第二电阻R2分压,保持在高电平。

一种在线更新BIOS的ROM写保护的系统及方法

技术领域

[0001] 本发明涉及通用服务器领域FW的写保护方法,具体提出一种在线更新BIOS的ROM写保护的系统及方法。

背景技术

[0002] BIOS是Basic Input/Output Operation System缩写,这个基本输入输出操作系统烧录在一个电可擦除的ROM中。称为BIOS的ROM。

[0003] 当服务器需要升级BIOS的时候,可以直接输入指令对ROM进行擦除和再写入。但是机器正常使用中有可能会出现偶然的错误指令,导致BIOS的ROM被误擦除,破坏BIOS文件,导致系统无法开机。

[0004] 因此,ROM厂商在芯片设计时都有预留一个写保护Pin。写保护Pin的电压准位是低电位的时候,无法通过指令来对BIOS的ROM进行擦除或写入的操作,只能把ROM从机器中取出来,使用特定的烧录器才能进行BIOS升级。

[0005] 当前设计方案主要有2种:(1)将写保护pin接地。此时ROM处于写保护状态,无法通过指令进行BIOS升级。(2)将写保护pin接电源。此时ROM处于解除写保护状态,可以通过指令升级BIOS,但是无写保护功能。

[0006] 目前,两种方案均不能实现既有写保护,又可在线更新功能需求。

发明内容

[0007] 本发明为解决上述问题,为此,本发明提供一种在线更新BIOS的ROM写保护的系统及方法,它具有实现既有写保护,又可在线更新功能需求的优点。

[0008] 为了实现上述目的,本发明采用如下技术方案。

[0009] 一种在线更新BIOS的ROM写保护的系统,包括,依次连接的电源端VCC、第一电阻R1、开关模块U1、第二电阻R2、地端GND。BIOS的ROM的写保护管脚WP#连接于开关模块U1和第二电阻R2之间。开关模块U1与控制器件连接,并能根据控制器件的指令控制第一电阻R1、第二电阻R2的连接或断开。第一电阻R1与第二电阻R2分压能使写保护管脚WP#处于无效状态。

[0010] 优选的,开关模块默认U1为断开状态。

[0011] 优选的,控制器件是BIOS、BMC、CPLD中的一种。

[0012] 优选的,第一电阻R1阻值为1k欧姆,第二电阻R2阻值为20k欧姆。

[0013] 一种在线更新BIOS的ROM写保护的方法,在正常使用状中,开关模块U1断开,BIOS的ROM的写保护管脚WP#通过电阻接地,写保护管脚WP#低电位有效,此时ROM不能被操作指令擦除或写入;需要写BIOS的ROM时,控制器件发出中断请求信号,使开关模块U1导通,此时写保护管脚WP#通过第一电阻R1和第二电阻R2分压,使BIOS的ROM的写保护管脚WP#仍然保持在高电平,写保护无效,此时可以进行刷新或者擦除ROM操作。

[0014] 本发明的有益效果:在不影响在线维护和DEBUG的基础上,使BIOS的ROM大部分时间处于写保护状态,不被操作指令误擦除或者写入,保持ROM文件的完整,提升系统稳定性,

解决因为BIOS的ROM被改写或者擦除引起的不开机故障。

附图说明

[0015] 图1是实施例的连接示意图。

具体实施方式

[0016] 下面结合附图与实施例对本发明作进一步说明。

[0017] 如图1所示,在线更新BIOS的ROM写保护的系统,包括,依次连接的电源端VCC、第一电阻R1、开关模块U1、第二电阻R2、地端GND。BIOS的ROM的写保护管脚WP#连接于开关模块U1和第二电阻R2之间。开关模块U1与控制器件连接,并能根据控制器件的指令控制第一电阻R1、第二电阻R2的连接或断开。第一电阻R1与第二电阻R2分压能使写保护管脚WP#处于无效状态。开关模块默认U1为断开状态。控制器件是BIOS、BMC、CPLD中的一种。第一电阻R1阻值为1k欧姆,第二电阻R2阻值为20k欧姆。

[0018] 在线更新BIOS的ROM写保护的方法,在正常使用状中,开关模块U1断开,BIOS的ROM的写保护管脚WP#通过第二电阻R2接地,写保护管脚WP#低电位有效,此时ROM不能被操作指令擦除或写入。

[0019] 当维护或者Debug时,BIOS/BMC/CPLD等控制器件发出中断请求信号,使开关模块U1导通,此时写保护管脚WP#通过第一电阻R1和第二电阻R2的电阻分压,使该脚位仍然保持高电平, $3.3V \times 20/21 = 3.14V$,写保护无效,此时可以进行刷新或者擦除ROM操作。

[0020] 上述虽然结合附图对本发明的具体实施方式进行了描述,但并非对本发明保护范围的限制,所属领域技术人员应该明白,在本发明的技术方案的基础上,本领域技术人员不需要付出创造性劳动即可做出的各种修改或变形仍在本发明的保护范围以内。

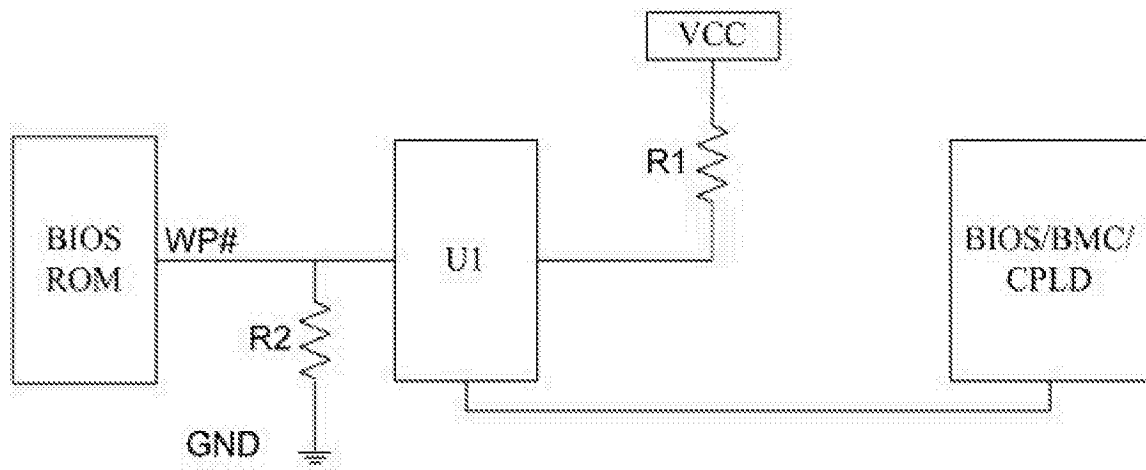


图1